THE DEGREE OF KUMMER EXTENSIONS OF NUMBER FIELDS

ANTONELLA PERUCCA, PIETRO SGOBBA AND SEBASTIANO TRONTO

ABSTRACT. Let K be a number field, and let ℓ be a prime number. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. We present an algorithm to compute the degree of the Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ over $K(\zeta_{\ell^m})$, where $n_1, \dots, n_r$ vary over the non-negative integers, m is an integer such that $m \geqslant \max(n_1, \dots, n_r)$. The output of the algorithm are formulas in the variables $n_1, \dots, n_r, m$ involving only a finite case distinction.

1. INTRODUCTION

If K is a number field, we are interested in cyclotomic-Kummer extensions of K. More precisely, let ℓ be a prime number, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. Then we are interested in the degree of the Kummer extension

$$K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})/K(\zeta_{\ell^m}), \tag{1}$$

where $n_1, \dots, n_r$ are non-negative integers, m is an integer such that $m \geqslant \max(n_1, \dots, n_r)$, and ζ_{ℓ^m} denotes a primitive ℓ^m-th root of unity. For fixed $n_1, \dots, n_r$ we can write (1) as

$$K\left(\zeta_{\ell^m}, \sqrt[\ell^n]{\alpha_1^{\ell^{n-n_1}}}, \dots, \sqrt[\ell^n]{\alpha_r^{\ell^{n-n_r}}}\right)/K(\zeta_{\ell^m}),$$

where $n = \max(n_1, \dots, n_r)$. So we may reduce to the case where all exponents $n_1, \dots, n_r$ are the same. The degree in this case is known by results of Debry and the first author [1], see Lemma 7. However, this strategy works only if we consider one single r-tuple $n_1, \dots, n_r$ because the elements of which we take the ℓ^n-th roots depend on $n_1, \dots, n_r$. Notice that if $K = \mathbb{Q}$ and $n_1, \dots, n_r$ are fixed, the computation of the degree of (1) was also achieved in [3, Theorem 4.2]. Also notice that if the rank r equals 2, then the author was able to produce formulas for all n_1, n_2, m where $m \geqslant \max(n_1, n_2)$ with a different method, see [4, 5].

What we achieve in this paper is computing, for any rank r, the degree of (1) for *all* exponents $n_1, \dots, n_r, m$ such that $m \geqslant \max(n_1, \dots, n_r)$. We present an algorithm whose output are formulas for the degree of (1) in the variables $n_1, \dots, n_r, m$ involving only a finite case distinction. The theoretical result which is the core of the algorithm is the following (where v_ℓ denotes the ℓ-adic valuation – recall that the considered Kummer degrees are a power of ℓ):

Theorem 1. *Let K be a number field, and let ℓ be a prime number. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. Let*

2010 *Mathematics Subject Classification.* Primary: 11Y40; Secondary: 11R20, 11R21.
Key words and phrases. Number field, Kummer theory, Kummer extension, degree.

$I = \{1, \dots, r\}$. *There is a computable non-negative integer s (which depends only on K, ℓ, and $\alpha_1, \dots, \alpha_r$) such that if $n_1, \dots, n_r, m$ are integers with $m \geqslant \max_{i \in I}(n_i)$, then we have*

$$v_\ell[K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i} : i \in I) : K(\zeta_{\ell^m}, \sqrt[\ell^{\min(n_i,s)}]{\alpha_i} : i \in I)] = \sum_{i=1}^{r} \max(n_i - s, 0)\,. \tag{2}$$

This result allows us to reduce the computation of the degree to the case in which all exponents $n_1, \dots, n_r$ are at most some computable constant s. In this way we are left to compute finitely many Kummer degrees.

The above result can be interpreted as an "eventual maximal growth" for the Kummer extension (1): if the exponents $n_1, \dots, n_r$ are sufficiently large then increasing one of them by 1 has the effect that the Kummer degree grows by a factor of ℓ. Moreover we can speak of "bounded failure of maximality" for the degree of the Kummer extension (1), in the sense of the following result:

Corollary 2. *Let K be a number field, and let ℓ be a prime number. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. There is a computable non-negative integer B (which depends only on K, ℓ, and $\alpha_1, \dots, \alpha_r$) such that*

$$\frac{\prod_{i=1}^{r} \ell^{n_i}}{[K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i} : i \in I) : K(\zeta_{\ell^m})]} \mid B$$

for all non-negative integers $n_1, \dots, n_r, m$ with $m \geqslant \max(n_1, \dots, n_r)$.

The structure of the paper is the following: in Section 2 we collect preliminary results, in Section 3 we prove Theorem 1 and its corollary, and in Section 4 we present the algorithm and make some examples of computations.

2. Preliminaries

2.1. **Linearly disjoint fields.** Let K be a number field. We say that two finite field extensions F and L of K (contained in one same field) are *linearly disjoint* over K if elements of F which are K-linearly independent are also L-linearly independent. This definition is the same as requiring that the following equality holds:

$$[F : K] \cdot [L : K] = [FL : K]\,.$$

We say that finitely many field extensions $F_1, \dots, F_r$ of K (contained in one same field) are *linearly disjoint* over K if each of these extensions is linearly disjoint from the compositum of the remaining ones (in other words, if for every $i = 1, \dots, r$ the field F_i is linearly disjoint from $F_1 \cdots \cancel{F_i} \cdots F_r$). Notice that this condition is stronger than requiring the extensions to be pairwise linearly disjoint (consider for example the three quadratic extensions of $\mathbb{Q}$ generated by $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ respectively). The condition is the same as requiring that the following equality holds:

$$\prod_{i=1}^{r} [F_i : K] = [F_1 \cdots F_r : K]\,.$$

Lemma 3. *Let K be a number field, and let $F_1, \dots, F_r$ be extensions of K which are linearly disjoint over K. For every $i = 1, \dots, r$ let F_i' be a subextension of F_i/K. Then the extensions $F_1', \dots, F_r'$ are also linearly disjoint over K.*

Proof. We know that for every $i = 1, \dots, r$ the field $F := F_i$ is linearly disjoint from $L := F_1 \cdots \cancel{F_i} \cdots F_r$. We need to show that for every $i = 1, \dots, r$ the field $F' := F_i'$ is linearly disjoint from $L' := F_1' \cdots \cancel{F_i'} \cdots F_r'$. We have thus reduced the assertion to considering only two fields: prove that if F and L are two extensions of K that are linearly disjoint over K, the same holds for two subextensions $F' \subseteq F$ and $L' \subseteq L$. Consider a subset of F' consisting of K-linearly independent elements. Since this is also a subset of F, we deduce that the elements are L-linearly independent, and in particular also L'-linearly independent. □

2.2. **Results from Kummer theory.**

Lemma 4. *Let K be a number field, and let ℓ be a prime number. Consider algebraic numbers $\alpha_1, \dots, \alpha_r$ in $K^\times$. Let $n_1, \dots, n_r, m$ be non-negative integers such that $m \geqslant \max(n_1, \dots, n_r)$. Then the degree of $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ over $K(\zeta_{\ell^m})$ divides $\prod_{i=1}^r \ell^{n_i}$. Moreover, equality holds if and only if the fields $K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i})$ are linearly disjoint over $K(\zeta_{\ell^m})$ and their degree over $K(\zeta_{\ell^m})$ equals ℓ^{n_i} for every i.*

Proof. For the first assertion, it suffices to notice that $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ is the compositum of the fields $K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i})$ for $i = 1, \dots, r$, and each of them has degree over $K(\zeta_{\ell^m})$ dividing ℓ^{n_i} (by considering the defining polynomial $x^{\ell^{n_i}} - \alpha_i$).

By the first assertion, the degree of the extension $K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i})/K(\zeta_{\ell^m})$ divides ℓ^{n_i}. So the degree of their compositum equals $\prod_{i=1}^r \ell^{n_i}$ if and only if the extensions are linearly disjoint and their degree equals ℓ^{n_i} for every i. □

Lemma 5. *Let K be a number field, and let ℓ be a prime number. Consider algebraic numbers $\alpha_1, \dots, \alpha_r$ in $K^\times$. Let $N_1, \dots, N_r, M$ be non-negative integers such that $M \geqslant \max(N_1, \dots, N_r)$. If we have*

$$[K(\zeta_{\ell^M}, \sqrt[\ell^{N_1}]{\alpha_1}, \dots, \sqrt[\ell^{N_r}]{\alpha_r}) : K(\zeta_{\ell^M})] = \prod_{i=1}^r \ell^{N_i},$$

then we also have

$$[K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^m})] = \prod_{i=1}^r \ell^{n_i}$$

for all non-negative integers $n_1, \dots, n_r, m$ such that $n_i \leqslant N_i$ for every $i = 1, \dots, r$ and such that $\max(n_1, \dots, n_r) \leqslant m \leqslant M$.

Proof. By Lemma 4 the extensions $K(\zeta_{\ell^M}, \sqrt[\ell^{N_i}]{\alpha_i})$ for $i = 1, \dots, r$ are linearly disjoint over $K(\zeta_{\ell^M})$ and each one has maximal degree ℓ^{N_i}.

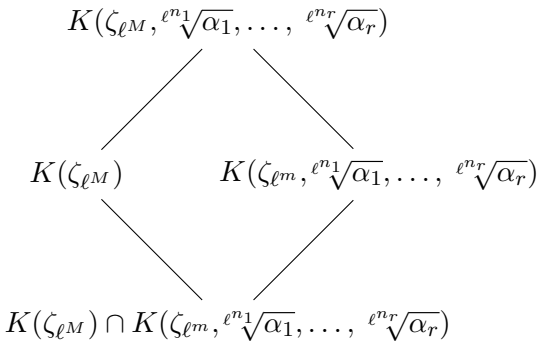
For each $i = 1, \dots, r$ consider the tower of fields $F_0 \subseteq F_1 \subseteq F_2$ with

$$F_0 := K(\zeta_{\ell^M}) \qquad F_1 := F_0(\sqrt[\ell^{n_i}]{\alpha_i}) \qquad F_2 := F_0(\sqrt[\ell^{N_i}]{\alpha_i}).$$

The degree of F_1/F_0 divides ℓ^{n_i} (just consider the defining polynomial $x^{\ell^{n_i}} - \alpha_i$). By writing $\beta_i := \sqrt[\ell^{n_i}]{\alpha_i}$ we have $F_2 = F_1(\sqrt[\ell^{N_i-n_i}]{\beta_i})$ and hence the degree of F_2/F_1 divides $\ell^{N_i-n_i}$. Since the degree of F_2/F_0 is ℓ^{N_i}, we deduce that the degree of F_1/F_0 is maximal, in other words that the degree of $K(\zeta_{\ell^M}, \sqrt[\ell^{n_i}]{\alpha_i})$ over $K(\zeta_{\ell^M})$ equals ℓ^{n_i}. By Lemma 3 also the extensions $K(\zeta_{\ell^M}, \sqrt[\ell^{n_i}]{\alpha_i})$ for $i = 1, \dots, r$ are linearly disjoint over $K(\zeta_{\ell^M})$, so we have

$$[K(\zeta_{\ell^M}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^M})] = \prod_{i=1}^{r} \ell^{n_i}\,.$$

Consider the following field diagram:



By Galois theory [2, Theorem 1.12 of Chapter VI] we deduce that the degree of the field $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ over its intersection with $K(\zeta_{\ell^M})$ has also degree $\prod_{i=1}^{r} \ell^{n_i}$. This implies by Lemma 4 that the degree of $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ over $K(\zeta_{\ell^m})$ is $\prod_{i=1}^{r} \ell^{n_i}$. □

3. Results on the degree of Kummer extensions

3.1. **Notation.** Let K be a number field, and let ℓ be a prime number. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup G of $K^\times$ of positive rank r. For every non-negative integers n and m with $m \geqslant n$ write $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})$ for the cyclotomic-Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^n]{\alpha_1}, \dots, \sqrt[\ell^n]{\alpha_r})$. Recall from [1, Section 3] that we may associate to G some computable non-negative integers $(d_1, \dots, d_r; h_1, \dots, h_r)$ which we call *ℓ-divisibility parameters* of G in K (the parameters $d_1, \dots, d_r$ are unique up to reordering, while there is some freedom in choosing $h_1, \dots, h_r$, see [1, Appendix]). The ℓ-divisibility parameters are computable, see [1, Section 6.1].

Notice that the degree of the Kummer extensions that we consider are powers of ℓ, so it suffices to evaluate the ℓ-adic valuation of their degree.

3.2. Results if the exponents $n_1, \dots, n_r$ are equal.

Theorem 6 ([1, Theorem 18])**.** *Suppose that ℓ is odd or that $\zeta_4 \in K$. Let $\omega \geqslant 1$ be the greatest integer satisfying $K(\zeta_\ell) = K(\zeta_{\ell^\omega})$. Let m and n be positive integers such that $m \geqslant$*

$\max(n,\omega)$. *Then we have*

$$(3)\quad v_\ell\left[K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}) : K(\zeta_{\ell^m})\right] = \max_{i=1,\dots,r}(h_i+\min(n,d_i)-m,0)+\sum_{i=1}^{r}\max(n-d_i,0)\,,$$

where $(d_1,\dots,d_r;h_1,\dots,h_r)$ *are* ℓ*-divisibility parameters of* G *in* K.

Lemma 7. *There are formulas for the Kummer degree*

$$[K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}) : K(\zeta_{\ell^m})]$$

for every non-negative integers m,n *such that* $m\geqslant n$*: the formulas involve only finitely many computable parameters (expressing properties of* G *over* K*) and a finite case distinction.*

Proof. If ℓ is odd or that $\zeta_4\in K$ it suffices to take the formula provided by Theorem 6 (because $m\geqslant\omega$ without loss of generality, the case $m=0$ being trivial). Now suppose that $\ell=2$ and $\zeta_4\in K$. If $m\geqslant 2$ we can extend the base field to $K(\zeta_4)$ and reduce to the previous case (notice that in [7] we proved that the 2-divisibility parameters of G over $K(\zeta_4)$ are determined by properties over K). We are left to compute the degree $[K(\sqrt{G}) : K]$, and this can be achieved with [1, Lemma 19]. □

Lemma 8. *There is a computable integer* s *such that for every* $m\geqslant n\geqslant s$ *we have*

$$(4)\qquad [K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}) : K(\zeta_{\ell^m})] = \ell^{r(n-s)}[K(\zeta_{\ell^m},\ \sqrt[\ell^s]{G}) : K(\zeta_{\ell^m})]\,.$$

Proof. If $\ell=2$ and $\zeta_4\notin K$ we take $s\geqslant 2$ so that the Kummer degrees can be computed by Theorem 6. By (3) we may then take

$$(5)\qquad s=\max_{i=1,\dots,r}(\varepsilon,h_i+d_i)\,,$$

where $\varepsilon=0$ if $\ell\neq 2$ or $\zeta_4\in K$, and $\varepsilon=2$ otherwise, and where $(d_1,\dots,d_r;h_1,\dots,h_r)$ are the ℓ-divisibility parameters of G over K (respectively, over $K(\zeta_4)$ if $\ell=2$ and $\zeta_4\notin K$). □

Notice that if G has rank 1, then there are easier formulas for the degree of $K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G})$ over $K(\zeta_{\ell^m})$, see [6, Section 4].

3.3. **Results for the algorithm.**

Theorem 9. *Let* K *be a number field, and let* ℓ *be a prime number. Consider elements* $\alpha_1,\dots,\alpha_r$ *of* $K^\times$ *which generate a torsion-free subgroup of* $K^\times$ *of positive rank* r*. There is a computable non-negative integer* s *(which depends only on* K*,* ℓ*, and* $\alpha_1,\dots,\alpha_r$*) such that if* $n_1,\dots,n_r,m$ *are integers with* $\min(n_1,\dots,n_r)\geqslant s$ *and* $m\geqslant\max(n_1,\dots,n_r)$*, then we have*

$$(6)\qquad v_\ell[K(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\ \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^m},\ \sqrt[\ell^s]{\alpha_1},\dots,\ \sqrt[\ell^s]{\alpha_r})] = \sum_{i=1}^{r}(n_i-s)\,.$$

Proof. Let s be as in Lemma 8, where $G=\langle\alpha_1,\dots,\alpha_r\rangle$. Then for every non-negative integers n,m with $m\geqslant n\geqslant s$ we have

$$[K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}) : K(\zeta_{\ell^m},\ \sqrt[\ell^s]{G})] = \ell^{r(n-s)}\,.$$

Set $F = K(\zeta_{\ell^m}, \sqrt[\ell^s]{G})$, and write $\beta_i = \sqrt[\ell^s]{\alpha_i}$. We can rewrite the above formula as

$$[F(\sqrt[\ell^{n-s}]{\beta_1}, \dots, \sqrt[\ell^{n-s}]{\beta_r}) : F] = \ell^{r(n-s)}\,. \tag{7}$$

Now let $n_1, \dots, n_r, m$ be integers with $\min(n_1, \dots, n_r) \geqslant s$ and $m \geqslant \max(n_1, \dots, n_r)$. Set $n = \max(n_1, \dots, n_r)$. Formula (7) says by Lemma 4 that the Kummer extension

$$F(\sqrt[\ell^{n-s}]{\beta_1}, \dots, \sqrt[\ell^{n-s}]{\beta_r})/F$$

has maximal degree. Then by Lemma 5 we deduce that

$$[F(\sqrt[\ell^{n_1-s}]{\beta_1}, \dots, \sqrt[\ell^{n_r-s}]{\beta_r}) : F] = \prod_{i=1}^{r} \ell^{n_i - s_i}. \tag{8}$$

The statement immediately follows from (8) by taking the ℓ-adic valuation of the degree. □

Remark 10. *In Theorem 9 the integer s can be taken as in Lemma 8 where $G = \langle \alpha_1, \dots, \alpha_r \rangle$. This is mentioned in the proof of Theorem 9.*

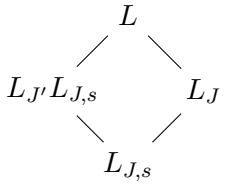
Theorem 11. *Let K be a number field, and let ℓ be a prime number. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. Let s be as in Theorem 9. Let $n_1, \dots, n_r, m$ be integers with $m \geqslant \max(n_1, \dots, n_r)$. Let J, J' be a partition of $\{1, \dots, r\}$ such that $n_j \geqslant s$ for all $j \in J$ and $n_i \leqslant s$ for all $i \in J'$. Then we have*

$$\begin{aligned} &v_\ell[K(\zeta_{\ell^m}, \sqrt[\ell^{n_j}]{\alpha_j}, \sqrt[\ell^{n_i}]{\alpha_i} : j \in J, i \in J') : K(\zeta_{\ell^m})] = \\ &v_\ell[K(\zeta_{\ell^m}, \sqrt[\ell^s]{\alpha_j}, \sqrt[\ell^{n_i}]{\alpha_i} : j \in J, i \in J') : K(\zeta_{\ell^m})] + \sum_{j \in J} (n_j - s)\,. \end{aligned}$$

Proof. We make use of the following notation:

$$\begin{aligned} L_J &= K(\zeta_{\ell^m}, \sqrt[\ell^{n_j}]{\alpha_j} : j \in J) \\ L_{J'} &= K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i} : i \in J') \\ L_{J,s} &= K(\zeta_{\ell^m}, \sqrt[\ell^s]{\alpha_j} : j \in J) \\ L_{J',s} &= K(\zeta_{\ell^m}, \sqrt[\ell^s]{\alpha_i} : i \in J') \\ L &= L_J L_{J'}\,. \end{aligned}$$

Consider the field extensions



We first prove the equality

$$[L : L_{J'} L_{J,s}] = [L_J : L_{J,s}]\,. \tag{9}$$

Clearly we have the inequalities

$$[L_J : L_{J,s}] \geqslant [L : L_{J'} L_{J,s}] \geqslant [L_{J',s} L_J : L_{J',s} L_{J,s}]\,, \tag{10}$$

because in the first inequality we are composing the extension with $L_{J'}$, while in the second inequality with $L_{J',s} \supseteq L_{J'}$. By Theorem 9 (applied by setting $n_i = s$ for all $i \in J'$), the degree on the right of (10) equals $\prod_{j\in J} \ell^{n_j - s}$ and it is maximal. We deduce that equalities hold in (10). In particular, we have shown that all three extensions have maximal degree, and we have proven (9). We then have

$$\begin{aligned}[L : K(\zeta_{\ell^m})] &= [L : L_{J'}L_{J,s}] \cdot [L_{J'}L_{J,s} : K(\zeta_{\ell^m})] \\ &= \prod_{j\in J} \ell^{n_j - s} \cdot [L_{J'}L_{J,s} : K(\zeta_{\ell^m})]\,,\end{aligned}$$

The statement follows by considering the ℓ-adic valuation of the above degrees. □

Proof of Theorem 1. Theorem 1 is a reformulation of Theorem 11. □

Remark 12. *With the notation of Theorem 1, we have proven in particular that there is a computable non-negative integer s such that*

$$\frac{\prod_{i=1}^r \ell^{n_i}}{[K(\zeta_{\ell^m},\ \sqrt[\ell^{n_i}]{\alpha_i} : i \in I) : K(\zeta_{\ell^m})]} = \frac{\prod_{i=1}^r \ell^{\min(n_i,s)}}{[K(\zeta_{\ell^m},\ \sqrt[\ell^{\min(n_i,s)}]{\alpha_i} : i \in I) : K(\zeta_{\ell^m})]}$$

holds for every non-negative integers $m, n_1, \dots, n_r$ with $m \geqslant \max(n_1, \dots, n_r)$.

Proof of Corollary 2. By Theorem 1 (and Remark 12) it suffices to have

$$\frac{\prod_{i=1}^r \ell^{\min(n_i,s)}}{[K(\zeta_{\ell^m},\ \sqrt[\ell^{\min(n_i,s)}]{\alpha_i} : i \in I) : K(\zeta_{\ell^m})]} \mid B$$

so we can take $B = \ell^{rs}$, which is computable by Remark 10. □

Remark 13. *Notice that in Corollary 2 we can take $B = \ell^{rs}$ (as stated in the proof) and that this bound is in general optimal. Indeed, for the case $\ell \neq 2$ or $\zeta_4 \in K$ it suffices to consider ℓ^s-th powers of strongly-ℓ-independent elements of K (as in* [1, Definition 10]*), so that the ℓ-divisibility parameters in* (5) *are $h_i = 0$ and $d_i = s$ for all $i = 1, \dots, r$.*

4. Computation of Kummer degrees

4.1. **The algorithm.** Let K be a number field, and let ℓ be a prime number. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. We present an algorithm to compute the degree of the Kummer extension

$$K(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1}, \dots,\ \sqrt[\ell^{n_r}]{\alpha_r})/K(\zeta_{\ell^m})\,, \tag{11}$$

where $n_1, \dots, n_r$ vary over the non-negative integers, and m is an integer such that $m \geqslant \max(n_1, \dots, n_r)$. The output of the algorithm are formulas in the variables $n_1, \dots, n_r, m$ involving only a finite case distinction.

By Theorem 1 with a finite case distinction we reduce to the case where $\max(n_1, \dots, n_r) \leqslant s$, where s is a computable non-negative integer depending only on $K, \ell, \alpha_1, \dots, \alpha_r$. Now fix one of the finitely many r-tuples $(n_1, \dots, n_r)$ of non-negative integers which are at most s. We can write (11) as

$$K\Big(\zeta_{\ell^m},\ \sqrt[\ell^n]{\alpha_1^{\ell^{n-n_1}}}, \dots,\ \sqrt[\ell^n]{\alpha_r^{\ell^{n-n_r}}}\Big)/K(\zeta_{\ell^m})\,,$$

where $n = \max(n_1, \dots, n_r)$. By setting $G = \langle \alpha_i^{\ell^{n-n_i}} : i \in I \rangle$ we have the extension

$$K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m}),$$

whose degree can be computed by Lemma 7 (see the proof of this lemma for details).

4.2. **Examples.**

Example 14. Let $K = \mathbb{Q}$ and $\ell = 3$. Consider the elements $\alpha_1 = 2$, $\alpha_2 = 3$, and $\alpha_3 = 5$. The 3-divisibility parameters of the group $G = \langle 2, 3, 5 \rangle$ over $\mathbb{Q}$ are all zero (see [1, Section 6.1]) so by (5) we can take $s = 0$ in Lemma 8 and hence also in Theorems 9 and 11. We deduce that we have

$$[K(\zeta_{3^m}, \sqrt[3^{n_1}]{2}, \sqrt[3^{n_2}]{3}, \sqrt[3^{n_3}]{5}) : K(\zeta_{3^m})] = 3^{n_1+n_2+n_3}$$

for all non-negative integers m, n_1, n_2, n_3 with $m \geqslant \max(n_1, n_2, n_3)$.

Generalizations of the above example are the following two remarks:

Remark 15. *Let K be a number field. Suppose that ℓ is odd or that $\zeta_4 \in K$. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. Let $G = \langle \alpha_1, \dots, \alpha_r \rangle$ be such that its ℓ-divisibility parameters are all zero (this means that $\alpha_1, \dots, \alpha_r$ are strongly-ℓ-independent in the sense of* [1, Definition 10]*). Then by* (5) *we can take $s = 0$ in Lemma 8 and hence also in Theorems 9 and 11. We deduce that we have*

$$[K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^m})] = \prod_{i=1}^{r} \ell^{n_i}$$

for all non-negative integers $m, n_1, \dots, n_r$ with $m \geqslant \max(n_1, \dots, n_r)$.

Remark 16. *Let K be a number field. Suppose that ℓ is odd or that $\zeta_4 \in K$. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. Suppose that $\alpha_i = \beta_i^{\ell^{d_i}}$ where $\beta_1, \dots, \beta_r$ are strongly-ℓ-independent elements of K. We have*

$$K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) = K(\zeta_{\ell^m}, \sqrt[\ell^{\max(n_1-d_1,0)}]{\beta_1}, \dots, \sqrt[\ell^{\max(n_r-d_r,0)}]{\beta_r}).$$

By the previous remark we conclude that

$$[K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^m})] = \prod_{i=1}^{r} \ell^{\max(n_i-d_i,0)}$$

for all non-negative integers $m, n_1, \dots, n_r$ with $m \geqslant \max(n_1, \dots, n_r)$.

Example 17. Let $K = \mathbb{Q}$ and $\ell = 2$. Consider the elements $\alpha_1 = -4$, $\alpha_2 = 5$. The 2-divisibility parameters of the group $G = \langle -4, 5 \rangle$ over $\mathbb{Q}(\zeta_4)$ are $(d_1, d_2; h_1, h_2) = (2, 0; 0, 0)$ because $-4 = (1+i)^4$ (and $1+i$ generates a prime ideal hence it is strongly-2-indivisibile in the sense of [1, Definition 5]). Then by (5) we can take $s = 2$ in Lemma 8 and hence also in Theorems 9 and 11.

We get the following case distinction, where n_1, n_2, m are non-negative integers with $m \geqslant \max(n_1, n_2)$, and where $\deg(n_1, n_2, m)$ stands for the degree of $\mathbb{Q}(\zeta_{2^m}, \sqrt[2^{n_1}]{-4}, \sqrt[2^{n_2}]{5})$ over $\mathbb{Q}(\zeta_{2^m})$:

n_1	n_2	m	$\deg(n_1, n_2, m)$
0	0	$\geqslant 0$	1
1	0	1	2
1	0	$\geqslant 2$	1
0	1	1	2
0	1	$\geqslant 2$	2
1	1	1	4
1	1	$\geqslant 2$	2
$\geqslant 2$	0	$\geqslant 2$	2^{n_1-2}
$\geqslant 2$	1	$\geqslant 2$	2^{n_1-1}
0	$\geqslant 2$	$\geqslant 2$	2^{n_2}
1	$\geqslant 2$	$\geqslant 2$	2^{n_2}
$\geqslant 2$	$\geqslant 2$	$\geqslant 2$	$2^{n_1+n_2-2}$

We then get the following formulas, with only three cases:

(1) If $m = 0, 1$: $\deg(n_1, n_2, m) = 2^{n_1+n_2}$;
(2) If $m \geqslant 2$ and $n_1 = 0, 1$: $\deg(n_1, n_2, m) = 2^{n_2}$;
(3) If $m \geqslant 2$ and $n_1 \geqslant 2$: $\deg(n_1, n_2, m) = 2^{n_1+n_2-2}$.

Example 18. Let $K = \mathbb{Q}(\sqrt{5})$, and let $\ell = 3$. Consider the elements $\alpha_1 = 1 + \sqrt{5}$ and $\alpha_2 = 5\sqrt{5} + 25 = (\sqrt{5})^3\alpha_1$. The 3-divisibility parameters for the group $G = \langle \alpha_1, \alpha_2 \rangle$ can be read off a 3-good basis of G (namely a basis as in [1, Theorem 14]), which is in this case $\alpha_1 = 1 + \sqrt{5}$ and $\alpha_2/\alpha_1 = (\sqrt{5})^3$. Notice that $1 + \sqrt{5}$ and $\sqrt{5}$ are strongly-3-independent in the sense of [1, Definition 10] because they generate distinct prime ideals: the first element generates the prime ideal (2) while the second generates the prime ideal over 5, which ramifies in $\mathbb{Q}(\sqrt{5})$. So the 3-divisibility parameters of G are $(d_1, d_2; h_1, h_2) = (0, 1; 0, 0)$. By (5) we can take $s = 1$ in Lemma 8 and hence also in Theorems 9 and 11. We then have the following case distinction, where n_1, n_2, m are non-negative integers with $m \geqslant \max(n_1, n_2)$, and where $\deg(n_1, n_2, m)$ stands for the degree of $K(\zeta_{3^m}, \sqrt[3^{n_1}]{\alpha_1}, \sqrt[3^{n_2}]{\alpha_2})$ over $K(\zeta_{3^m})$:

n_1	n_2	m	$\deg(n_1, n_2, m)$
0	0	$\geqslant 0$	1
$\geqslant 1$	0	$\geqslant 0$	3^{n_1}
0	$\geqslant 1$	$\geqslant 0$	3^{n_2}
$\geqslant 1$	$\geqslant 1$	$\geqslant 0$	$3^{n_1+n_2-1}$

REFERENCES

[1] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.
[2] LANG, S, *Algebra*, Revised third edition, Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2002.
[3] PALENSTIJN, W. J., *Radicals in arithmetic*, PhD thesis, University of Leiden (2014), available on `https://openaccess.leidenuniv.nl/handle/1887/25833`.
[4] PERUCCA, A., *Kummer extensions of number fields (the case of rank 2)*, preprint available on ORBilu `https://orbilu.uni.lu/handle/10993/41552`.
[5] PERUCCA, A., *Kummer extensions of number fields (the case of rank 2) II*, preprint available on ORBilu `https://orbilu.uni.lu/handle/10993/41659`.

[6] PERUCCA, A., *The order of the reductions of an algebraic integer*, J. Number Theory, **148** (2015), 121–136.
[7] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Addendum to: Reductions of algebraic integers [J. Number Theory 167 (2016) 259–283]*, J. Number Theory **209** (2020), 391–395.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, 6 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: antonella.perucca@uni.lu, pietro.sgobba@uni.lu, sebastiano.tronto@uni.lu